McAfee®

personalfirewallplus

Manual del usuario



DERECHOS DE PROPIEDAD INTELECTUAL

ATRIBUCIONES DE MARCAS COMERCIALES

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (Y EN KATAKANA), ACTIVESHIELD, ANTIVIRUS ANYWARE AND DESIGN, CLEAN-UP, DESIGN (E ESTILIZADO), DESIGN (N ESTILIZADO), ENTERCEPT, ENTERPRISE SECURECAST, ENTERPRISE SECURECAST (Y EN KATAKANA), EPOLICY ORCHESTRATOR, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD, GROUPSHIELD (Y EN KATAKANA), GUARD DOG, HOMEGUARD, HUNTER, INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, M AND DESIGN, MCAFEE, MCAFEE (Y EN KATAKANA), MCAFEE AND DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NA NETWORK ASSOCIATES, NET TOOLS, NET TOOLS (Y EN KATAKANA), NETCRYPTO, NETOCTOPUS, NETSCAN, NETSHIELD, NETWORK ASSOCIATES, NETWORK ASSOCIATES COLLISEUM, NETXRAY, NOTESGUARD, NUTS & BOLTS, OIL CHANGE, PC MEDIC, PCNOTARY, PRIMESUPPORT, RINGFENCE, ROUTER PM, SECURECAST, SECURESELECT, SPAMKILLER, STALKER, THREATSCAN, TIS, TMEG, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (Y EN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (Y EN KATAKANA), WEBSTALKER, WEBWALL, WHAT'S THE STATE OF YOUR IDS?, WHO'S WATCHING YOUR NETWORK, YOUR E-BUSINESS DEFENDER, YOUR NETWORK. OUR BUSINESS. son marcas registradas o marcas comerciales de McAfee, Inc. o sus empresas filiales en los EE.UU. y otros países. El color rojo y la seguridad son los elementos distintivos de los productos de la marca McAfee. Todas las demás marcas comerciales, registradas y sin registrar, incluidas en el presente documento son propiedad exclusiva de sus respectivos titulares.

INFORMACIÓN SOBRE LA LICENCIA

Acuerdo de licencia

AVISO A TODOS LOS USUARIOS: LEA DETENIDAMENTE EL ACUERDO LEGAL APROPIADO CORRESPONDIENTE A LA LICENCIA ADQUIRIDA, QUE ESTABLECE LOS TÉRMINOS Y CONDICIONES GENERALES DE USO DEL SOFTWARE PARA EL QUE SE CONCEDE LA LICENCIA. SI NO SABE QUÉ TIPO DE LICENCIA HA ADQUIRIDO, CONSULTE LOS DOCUMENTOS DE VENTA Y OTROS DOCUMENTOS RELACIONADOS CON LA CONCESIÓN DE LA LICENCIA O CON LA ORDEN DE COMPRA QUE ACOMPAÑAN AL PAQUETE DE SOFTWARE O QUE HAYA RECIBIDO POR SEPARADO COMO PARTE DE LA COMPRA (POR EJEMPLO, UN MANUAL, UN ARCHIVO DEL CD DEL PRODUCTO O UN ARCHIVO DEL SITIO WEB DESDE EL QUE DESCARGÓ EL PAQUETE DE SOFTWARE). SI NO ESTÁ DE ACUERDO CON TODAS LAS CONDICIONES DESCRITAS EN EL ACUERDO, NO INSTALE EL SOFTWARE. SEGÚN CORRESPONDA, PUEDE DEVOLVER EL PRODUCTO A MCAFEE, INC. O AL ESTABLECIMIENTO DE COMPRA PARA QUE SE LE REEMBOLSE EL IMPORTE COMPLETO.

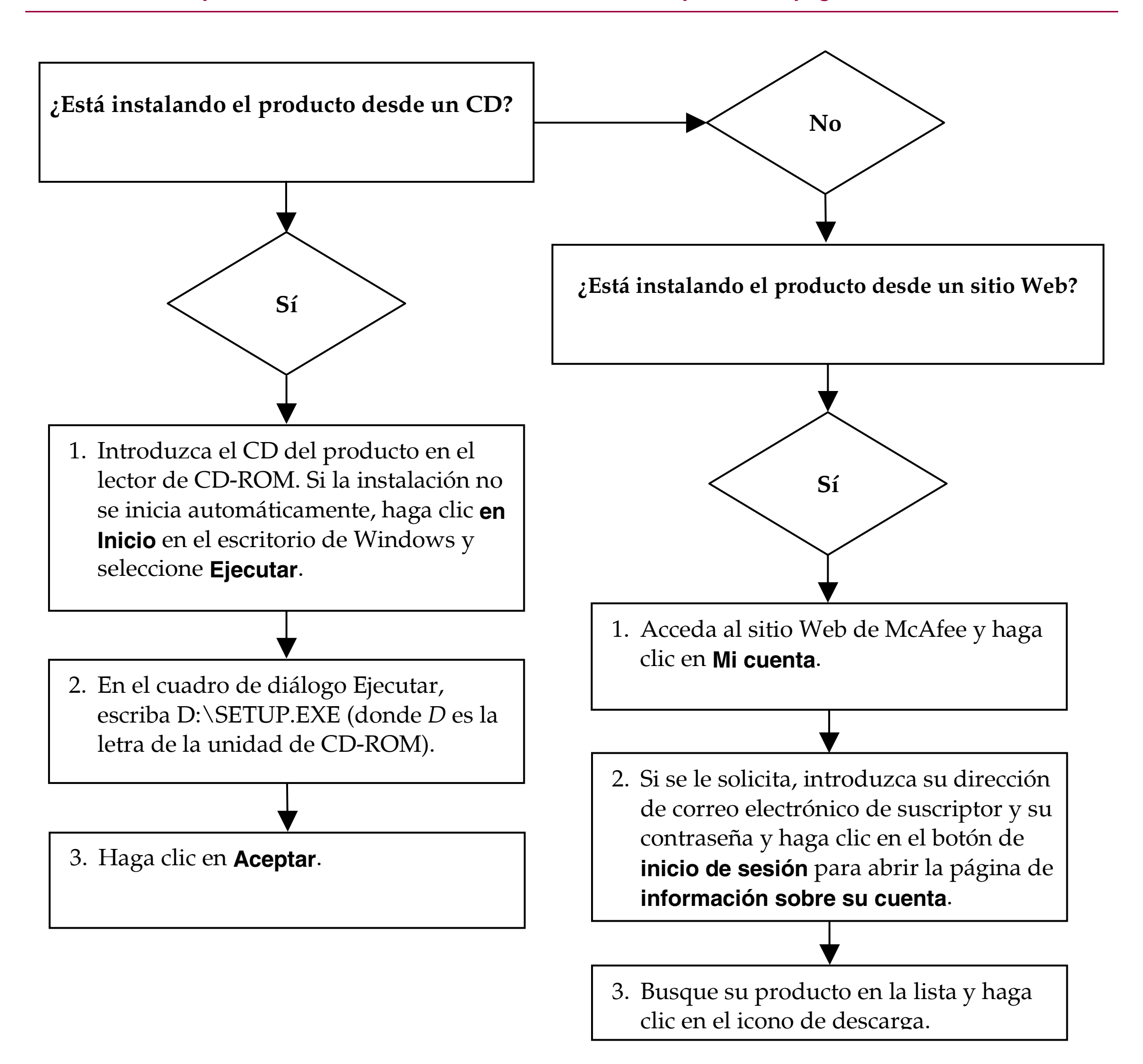
Atribuciones

Este producto incluye o puede incluir lo siguiente:

♦ Software desarrollado por OpenSSL Project para su uso en OpenSSL Toolkit (http://www.openssl.org/). ♦ Software criptográfico escrito por Eric A. Young y software escrito por Tim J. Hudson. ♦ Algunos programas de software que se conceden bajo licencia (o sublicencia) al usuario mediante licencia pública general (GPL) u otras licencias similares de software gratuito que, entre otros derechos, permiten al usuario copiar, modificar y redistribuir ciertos programas, o determinadas partes de ellos, así como acceder al código fuente. Esta licencia pública general requiere que cualquier software proporcionado con este tipo de licencia se distribuya en formato binario ejecutable y que el código fuente se ponga a disposición de estos usuarios. El código fuente del software con licencia pública general se incluye también en el CD. Si cualquier licencia de software gratuito requiere que McAfee, Inc. proporcione derechos de utilización, copia o modificación de un programa de software que sean más amplios que los aquí expuestos, tales derechos prevalecerán sobre los derechos y restricciones aquí expresados. ♦ Software escrito originalmente por Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer. ♦ Software escrito originalmente por Robert Nordier, Copyright © 1996-7 Robert Nordier. ♦ Software escrito por Douglas W. Sauder. ♦ Software desarrollado por la Apache Software Foundation (http://www.apache.org/). Puede encontrar una copia del acuerdo de licencia de este software en www.apache.org/licenses/LICENSE-2.0.txt. ♦ International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation y otros. ♦ Software desarrollado por CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc. ♦ Tecnología FEAD® Optimizer®, Copyright Netopsystems AG, Berlín, Alemania. ♦ Outside In® Viewer Technology © 1992-2001 Stellent Chicago, Inc. y/o Outside In® HTML Export, © 2001 Stellent Chicago, Inc. ♦ Software propiedad de Thai Open Source Software Center Ltd. y Clark Cooper, © 1998, 1999, 2000. ♦ Software propiedad de Expat maintainers. ♦ Software propiedad de The Regents of the University of California, © 1989. ♦ Software propiedad de Gunnar Ritter. ♦ Software propiedad de Sun Microsystems®, Inc.© 2003. ♦ Software propiedad de Gisle Aas. © 1995-2003. ♦ Software propiedad de Michael A. Chase, © 1999-2000. ♦ Software propiedad de Neil Winton, © 1995-1996. ♦ Software propiedad de RSA Data Security, Inc., © 1990-1992. ♦ Software propiedad de Sean M. Burke, © 1999, 2000. ♦ Software propiedad de Martijn Koster, © 1995. ♦ Software propiedad de Brad Appleton, © 1996-1999. ♦ Software propiedad de Michael G. Schwern, © 2001. ♦ Software propiedad de Graham Barr, © 1998. ♦ Software propiedad de Larry Wall y Clark Cooper, © 1998-2000. ♦ Software propiedad de Frodo Looijaard, © 1997. ♦ Software propiedad de Python Software Foundation, Copyright © 2001, 2002, 2003. Hay una copia del acuerdo de licencia para este software en www.python.org. ♦ Software propiedad de Beman Dawes, © 1994-1999, 2002. ♦ Software escrito por Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame. ♦ Software propiedad de Simone Bordet & Marco Cravero, © 2002. ♦ Software propiedad de Stephen Purcell, © 2001. ♦ Software desarrollado por Indiana University Extreme! Lab (http://www.extreme.indiana.edu/). ♦ Software propiedad de International Business Machines Corporation y otros, © 1995-2003. ♦ Software desarrollado por la University of California, Berkeley y sus donantes. ♦ Software desarrollado por Ralf S. Engelschall <rse@engelschall.com> para su uso en el proyecto the mod_ssl (http://www.modssl.org/). ♦ Software propiedad de Kevlin Henney, © 2000-2002. ♦ Software propiedad de Peter Dimov y Multi Media Ltd. © 2001, 2002. ♦ Software propiedad de David Abrahams, © 2001, 2002. Consulte http://www.boost.org/libs/bind/bind.html para obtener la documentación. ♦ Software propiedad de Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000. ♦ Software propiedad de Boost.org, © 1999-2002. ♦ Software propiedad de Nicolai M. Josuttis, © 1999. ♦ Software propiedad de Jeremy Siek, © 1999-2001. ♦ Software propiedad de Daryle Walker, © 2001. ♦ Software propiedad de Chuck Allison y Jeremy Siek, © 2001, 2002. ♦ Software propiedad de Samuel Krempp, © 2001. Consulte http://www.boost.org para obtener el historial de revisiones, actualizaciones y documentación. ♦ Software propiedad de Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002. ♦ Software propiedad de Cadenza New Zealand Ltd., © 2000. ♦ Software propiedad de Jens Maurer, © 2000, 2001. ♦ Software propiedad de Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000. ♦ Software propiedad de Ronald Garcia, © 2002. ♦ Software propiedad de David Abrahams, Jeremy Siek y Daryle Walker, © 1999-2001. ♦ Software propiedad de Stephen Cleary (shammah@voyager.net), © 2000. ♦ Software propiedad de Housemarque Oy <http://www.housemarque.com>, © 2001. ♦ Software propiedad de Paul Moore, © 1999. ♦ Software propiedad de Dr. John Maddock, © 1998-2002. ♦ Software propiedad de Greg Colvin y Beman Dawes, © 1998, 1999. ♦ Software propiedad de Peter Dimov, © 2001, 2002. ♦ Software propiedad de Jeremy Siek y John R. Bandela, © 2001. ♦ Software propiedad de Joerg Walter y Mathias Koch, © 2000-2002.

Tarjeta de inicio rápido

Si va a instalar el producto desde un CD o desde un sitio Web, imprima esta página de referencia.



Si desea obtener más información

Para ver los manuales de usuario del CD del producto, asegúrese de que tiene instalado Acrobat Reader; en caso contrario, instálelo ahora desde el CD del producto de McAfee.

1. Introduzca el CD del producto en la unidad de CD-ROM.
2. Abra el Explorador de Windows: Haga clic en **Inicio** en el escritorio de Windows y, a continuación, en **Buscar**.
3. Busque la carpeta Manuales y haga doble clic en el Manual del usuario en formato PDF que desee abrir.

Ventajas del registro

McAfee recomienda que siga los sencillos pasos en el producto para transmitir su registro directamente. Gracias al registro, podrá disfrutar de asistencia técnica especializada y puntual, así como de las ventajas siguientes:

- Soporte electrónico GRATUITO.
- Actualizaciones de los archivos de definición de virus (.DAT) durante un año a partir de la instalación tras la adquisición del software de VirusScan.

  Vaya a http://es.mcafee.com para obtener información sobre el precio de un año adicional de definiciones de virus.
- Una garantía de 60 días que le asegura la sustitución del software o CD si está defectuoso o dañado.
- Actualizaciones de filtros de SpamKiller durante un año después de instalarlo tras la adquisición del software SpamKiller.

  Vaya a http://es.mcafee.com para obtener información sobre el precio de un año adicional de actualizaciones de filtros.
- McAfee Internet Security Suite se actualiza durante un año después de la instalación cuando adquirió el software MIS.

  Vaya a http://es.mcafee.com para obtener información sobre el precio de un año adicional de actualizaciones de contenido.

Soporte técnico

Para obtener asistencia técnica, visite

http://www.mcafeeayuda.com/.

Nuestro sitio de soporte permite acceder durante las 24 horas del día al sencillo Asistente de respuestas para obtener soluciones a las preguntas de soporte más comunes.

Los usuarios experimentados también pueden utilizar las opciones avanzadas, que incluyen la búsqueda por palabras clave o el árbol de ayuda. Si no logra encontrar una solución a su problema, puede acceder a nuestros servicios GRATUITOS Chat Now! e E-mail Express! Estas opciones le ayudan a ponerse en contacto rápidamente con nuestros ingenieros cualificados de soporte técnico a través de Internet y sin coste alguno. También puede obtener información de soporte por teléfono en

http://www.mcafeeayuda.com/.

Contenido

Introducción 1

Bienvenido a McAfee Personal Firewall Plus.

El software McAfee Personal Firewall Plus ofrece protección avanzada para su ordenador y sus datos personales. Personal Firewall establece una barrera entre su equipo e Internet y controla en segundo plano si se realizan operaciones de tráfico de Internet que resulten sospechosas.

Gracias a él, disfrutará de las funciones siguientes:

- Protección contra potenciales ataques e intentos de ataque de los piratas informáticos.
- Complemento de defensas antivirus.
- Control de la actividad de Internet y de la red.
- Alerta contra eventos potencialmente hostiles.
- Información detallada sobre tráfico de Internet sospechoso.
- Integración con la funcionalidad Hackerwatch.org, que incluye la elaboración de informes de eventos, herramientas de autocomprobación y la posibilidad de enviar a las autoridades en línea los sucesos recibidos.
- Funciones de rastreo y búsqueda de eventos.

Funciones nuevas

- **Mejoras en soporte para juegos**
  McAfee Personal Firewall Plus protege su equipo de intentos de intrusión y actividades sospechosas en los juegos a toda pantalla, pero puede ocultar alertas si detecta intentos de intrusión o actividades sospechosas. Las alertas rojas aparecen después de salir del juego.
- **Mejoras en la gestión del acceso**
  McAfee Personal Firewall Plus permite a los usuarios conceder a las aplicaciones acceso temporal a Internet. El acceso se restringe al lapso de tiempo desde el momento en el que se inicia la aplicación hasta cuando se cierra. Cuando Personal Firewall detecta un programa desconocido, que trata de comunicarse con Internet, una Alerta roja ofrece la opción de conceder a la aplicación acceso temporal a Internet.

- **Mejoras en el control de la seguridad**
  Si se utiliza la función Bloqueado en McAfee Personal Firewall Plus podrá bloquear de manera instantánea todo el tráfico de Internet entrante y saliente entre su equipo e Internet. Los usuarios pueden activar o desactivar la función Bloqueado desde tres lugares diferentes de Personal Firewall.

- **Mejoras en las opciones de recuperación**
  Puede ejecutar Restablecer opciones para restablecer automáticamente la configuración predeterminada de Personal Firewall. Si Personal Firewall muestra un comportamiento extraño que no puede corregir, puede decidir cambiar la configuración actual y volver a la configuración predeterminada del producto.

- **Protección contra la conexión a Internet**
  Para impedir que un usuario desactive de manera accidental su conexión a Internet, la opción de prohibir una dirección de Internet se excluye de una Alerta azul cuando Personal Firewall detecta una conexión que se origina de un servidor DHCP o DNS. Si el tráfico entrante no se origina en un servidor DHCP o DNS, aparece la opción.

- **Integración mejorada con HackerWatch.org**
  Ahora resulta más fácil que nunca informar sobre posibles piratas informáticos. McAfee Personal Firewall Plus mejora la funcionalidad de HackerWatch.org, que incluye el envío de eventos potencialmente malintencionados a la base de datos.

- **Mejoras en la gestión inteligente de las aplicaciones**
  Cuando una aplicación pretende acceder a Internet, Personal Firewall comprueba en primer lugar si la reconoce como fiable o malintencionada. Si Personal Firewall reconoce la aplicación como fiable, permitirá automáticamente su acceso a Internet sin necesidad de la intervención del usuario.

- **Detección avanzada de troyanos**
  McAfee Personal Firewall Plus combina la administración de la conexión entre las aplicaciones con una base de datos mejorada para detectar y bloquear el acceso a Internet y la posible transmisión de sus datos personales a las aplicaciones potencialmente más peligrosas, como los troyanos.

- **Mejoras en el rastreo visual**
  Visual Trace incluye mapas gráficos de fácil lectura que muestran el origen del tráfico y de los ataques hostiles en todo el mundo, junto con información detallada sobre contactos y propietarios de las direcciones IP de origen.

- **Mayor facilidad de uso**
  McAfee Personal Firewall Plus incluye un Asistente para la configuración y un tutorial para guiar a los usuarios durante la configuración y utilización del cortafuegos. Aunque el producto está diseñado para su uso sin necesidad de intervención del usuario, McAfee ofrece a los usuarios un buen número de recursos para comprender y apreciar lo que el cortafuegos puede hacer por ellos.

- **Mejoras en la detección de intrusiones**
  El sistema de detección de intrusiones (IDS, Intrusion Detection System) de Personal Firewall detecta los patrones comunes de ataque y otras actividades sospechosas. La detección de intrusiones controla todos los paquetes de datos en busca de transferencias de datos o métodos de transferencia que resulten sospechosos, y los incluye en el registro de eventos.

- **Mejoras en el análisis del tráfico**
  McAfee Personal Firewall Plus permite que los usuarios vean tanto los datos que entran como los que salen de su equipo, y, además, muestra las conexiones de las aplicaciones, incluidas las que están "a la escucha" de conexiones abiertas. Esto permite a los usuarios ver y actuar sobre las aplicaciones que pudieran mostrarse susceptibles de intrusión.

Requisitos del sistema

- Microsoft® Windows 98, Windows Me, Windows 2000 o Windows XP
- Ordenador personal con procesador Pentium o compatible
  Windows 98, 2000: 133 MHz o superior
  Windows Me: 150 MHz o superior
  Windows XP (Home y Pro): 300 MHz o superior
- RAM
  Windows 98, Me, 2000: 64 MB
  Windows XP (Home y Pro): 128 MB
- 40 MB de espacio en el disco duro
- Microsoft® Internet Explorer 5.5 o superior

NOTA
Para obtener la última versión de Internet Explorer, visite el sitio Web de Microsoft en la dirección http://www.microsoft.com/.

Desinstalación de otros cortafuegos

Antes de instalar McAfee Personal Firewall, es necesario desinstalar cualquier otro programa cortafuegos que se encuentre instalado en el equipo. Para ello, siga las instrucciones de desinstalación del programa cortafuegos que tenga instalado.

NOTA
Si utiliza Windows XP, no es necesario que desactive la función de cortafuegos incorporada antes de instalar el McAfee Personal Firewall Plus. No obstante, recomendamos que desactive la función de cortafuegos incorporada. De no hacerlo, no recibirá eventos en el registro de eventos entrantes de McAfee Personal Firewall Plus.

Configuración del cortafuegos predeterminado

McAfee Personal Firewall puede gestionar permisos y tráfico para las aplicaciones de Internet de su equipo, aún cuando detecta que se está ejecutando Windows Firewall en éste.

Una vez instalado, McAfee Personal Firewall desactiva automáticamente Firewall de Windows y se establece como cortafuegos predeterminado. Entonces sólo podrá utilizar la funcionalidad y los mensajes de McAfee Personal Firewall. Si posteriormente activa Firewall de Windows a través de Windows Security Center o el Panel de control de Windows, al permitir que los dos cortafuegos se ejecuten en el equipo puede provocar una pérdida parcial del registro de McAfee Firewall, así como la duplicación del estado y de los mensajes de alerta.

NOTA
Si están activados los dos cortafuegos, McAfee Personal Firewall no muestra todas las direcciones IP bloqueadas en la ficha Eventos entrantes. Firewall de Windows intercepta la mayor parte de estos eventos y los bloquea, evitando que McAfee Personal Firewall detecte o registre dichos eventos. Sin embargo, es posible que McAfee Personal Firewall bloquee tráfico adicional en función de otros factores de seguridad, y quedará un registro de dicho tráfico.

El registro está desactivado en Firewall de Windows de forma predeterminada, pero si decide activar los dos cortafuegos, puede activar el registro de Firewall de Windows. El registro predeterminado de Firewall de Windows es C:\Windows\pfirewall.log

Para asegurarse de que el equipo está protegido al menos por un cortafuegos, Firewall de Windows se vuelve a activar automáticamente cuando se desinstala McAfee Personal Firewall.

Si desactiva McAfee Personal Firewall o establece el ajuste de seguridad como **Abierto** sin activar manualmente Firewall de Windows, se eliminará completamente la protección del cortafuegos excepto en el caso de las aplicaciones bloqueadas anteriormente.

Configuración del nivel de seguridad

Puede configurar las opciones de seguridad para indicar el modo en que Personal Firewall responderá cuando detecte tráfico no deseado. De forma predeterminada, se activa el nivel de seguridad **Estándar**. En el nivel de seguridad **Estándar**, cuando una aplicación solicita acceso a Internet y se le concede, le está otorgando Acceso pleno a la aplicación. El Acceso pleno permite a la aplicación enviar y recibir datos no solicitados desde un puerto que no sea del sistema.

Para configurar los ajustes de seguridad:

1 Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Opciones**.

2 Haga clic en el icono **Configuración de seguridad**.

3 Configure el nivel de seguridad moviendo el control deslizante hasta el valor deseado.

El rango de niveles de seguridad abarca desde Bloqueado a Abierto:

- **Bloqueado :** se cierran todas las conexiones a Internet del equipo. Puede utilizar esta opción para bloquear puertos que configuró para estar abiertos en la página Servicios del sistema.
- **Seguridad estricta :** cuando una aplicación solicita un tipo de acceso a Internet específico (por ejemplo, Sólo acceso saliente), puede permitir o no que la aplicación se conecte a Internet. Si la aplicación solicita más adelante Acceso pleno, puede concedérselo o restringirlo a Sólo acceso saliente.
- **Seguridad Estándar (recomendado) :** cuando una aplicación solicita y se le concede acceso a Internet, la aplicación disfruta de acceso pleno a Internet para gestionar el tráfico entrante y saliente.
- **Seguridad Fiable :** se confía automáticamente en todas las aplicaciones cuando intentan acceder por primera vez a Internet. Sin embargo, puede configurar Personal Firewall para utilizar alertas que le notifiquen sobre nuevas aplicaciones en su equipo. Utilice este valor si percibe que algunos juegos o medios de transferencia no funcionan.
- **Abierto :** el cortafuegos está desactivado. Este valor de configuración permite todo el tráfico a través de Personal Firewall sin ningún tipo de filtro.

NOTA
Las aplicaciones previamente bloqueadas siguen bloqueadas cuando el cortafuegos se configura con el valor de seguridad **Abierto** o **Bloqueado**. Para evitar esto, puede cambiar los permisos de las aplicaciones a **Permitir acceso pleno** o simplemente eliminar la regla del permiso **Bloqueado** en la lista **Aplicaciones de Internet**.

4 Seleccione configuración de seguridad adicional:

NOTA
Si su equipo dispone de Windows XP y se han agregado varios usuarios de XP, estas opciones están disponibles únicamente si se inicia la sesión como Administrador.

- **Registrar eventos de detección de intrusiones (IDS) en registro de eventos entrantes:** si selecciona esta opción, los eventos detectados por IDS aparecerán en el registro Eventos entrantes. El sistema de detección de intrusiones detecta los tipos de ataques comunes y otras actividades sospechosas. La detección de intrusiones controla todos los paquetes de datos entrantes y salientes en busca de transferencias de datos o métodos de transferencia sospechosos. Los compara con una base de datos de "definición" y se deshace de los paquetes procedentes del equipo infractor.

  IDS busca patrones de tráfico específicos utilizados por los que efectúan el ataque. IDS comprueba cada paquete que recibe el equipo para detectar tráfico sospechoso o de ataques conocidos. Por ejemplo, si Personal Firewall detecta paquetes de ICMP, los analiza en busca de patrones de tráfico sospechoso comparando el tráfico de ICMP con los patrones de los ataques conocidos.

- **Aceptar solicitudes de ping ICMP**: el tráfico de ICMP se usa principalmente para llevar a cabo seguimientos y hacer ping. Los ping se hacen habitualmente para realizar una comprobación rápida antes de intentar iniciar las comunicaciones. Si utiliza o ha utilizado un programa de intercambio de archivos, es posible que su equipo reciba numerosas solicitudes de ping. Si selecciona esta opción, Personal Firewall permite todas las solicitudes de ping sin registrarlas en el registro de eventos entrantes. Si no selecciona esta opción, Personal Firewall bloquea todas las solicitudes de ping y las registra en el registro de eventos entrantes.

- **Permitir a usuarios con derechos restringidos cambiar la configuración de Personal Firewall**: si el equipo dispone de Windows XP o Windows 2000 Professional con varios usuarios de XP, seleccione esta opción para permitir que los usuarios de XP restringidos modifiquen la configuración de Personal Firewall.

5. Haga clic en **Aceptar** cuando haya terminado de realizar cambios.

Comprobación de McAfee Personal Firewall Plus

Puede comprobar si la instalación de Personal Firewall presenta posibles puntos vulnerables a intrusiones o actividades sospechosas.

Para comprobar la instalación de Personal Firewall desde el icono de la bandeja del sistema de McAfee:

- Haga clic con el botón secundario en el icono de McAfee de la bandeja del sistema de Windows y seleccione **Comprobar cortafuegos**.

Personal Firewall abre Internet Explorer y se dirige a http://www.hackerwatch.org/, un sitio Web que mantiene McAfee. Siga las instrucciones de la página Hackerwatch.org para comprobar Personal Firewall.

Utilización de McAfee SecurityCenter

McAfee SecurityCenter es una herramienta de seguridad universal a la que puede acceder desde su icono situado en la bandeja del sistema de Windows o directamente desde el escritorio de Windows. Con ella puede realizar estas útiles tareas:

- Obtener un análisis de seguridad del equipo.
- Ejecutar, gestionar y configurar todas las suscripciones de McAfee desde el mismo icono.
- Ver alertas de virus actualizadas continuamente y la información más reciente sobre productos.
- Acceder rápidamente a las preguntas más frecuentes y a la información detallada de la cuenta en el sitio Web de McAfee.

NOTA
Si desea obtener más información sobre sus funciones, haga clic en **Ayuda** en el cuadro de diálogo **SecurityCenter**.

Cuando SecurityCenter se encuentra en ejecución y todas las funciones de McAfee están activadas en el equipo, aparecerá un icono con una M en color rojo en la bandeja del sistema de Windows. Esta área se encuentra normalmente en la esquina inferior derecha del escritorio de Windows e incluye el reloj.

Si alguna de las aplicaciones de McAfee instaladas se encuentra desactivada, el icono de McAfee aparecerá en color negro.

Para iniciar McAfee SecurityCenter:

1. Haga clic con el botón secundario en el icono de McAfee y, a continuación, seleccione **Abrir SecurityCenter**.

Para iniciar Personal Firewall desde McAfee SecurityCenter:

1. Desde SecurityCenter, haga clic en la ficha **Personal Firewall Plus**:
2. Seleccione una tarea en el menú Deseo.

Para iniciar Personal Firewall desde Windows:

1. Haga clic con el botón secundario en el icono de McAfee de la bandeja del sistema de Windows y señale **Personal Firewall**.
2. Seleccione la tarea.

Utilización de McAfee Personal Firewall Plus

2

Para abrir Personal Firewall:

- Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** , y seleccione una tarea.

Acerca de la página Resumen

El Resumen de Personal Firewall contiene cuatro páginas de resumen:

- Resumen principal
- Resumen de la aplicación
- Resumen de evento
- Resumen de HackerWatch

Las páginas de resumen contienen una serie de informes sobre los eventos entrantes recientes, el estado de las aplicaciones y la actividad de intrusión mundial recogida por HackerWatch.org. También encontrará vínculos sobre tareas comunes realizadas en Personal Firewall.

Para abrir la página Resumen principal en Personal Firewall:

- Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Ver resumen** (Figura 2-1).



Figura 2-1. Página Resumen principal

Haga clic en los siguientes vínculos para desplazarse a las páginas de resumen:

Elemento	Descripción
Cambiar vista	Haga clic en **Cambiar vista** para abrir una lista de páginas de resumen. Seleccione en la lista la página Resumen que desea ver.
Flecha derecha	Haga clic en el icono de flecha derecha para ver la siguiente página Resumen.
Flecha izquierda	Haga clic en el icono de flecha izquierda para ver la página Resumen anterior.
Inicio	Haga clic en el icono de inicio para volver a la página **Resumen principal**.

La página Resumen principal contiene los datos siguientes:

Elemento	Descripción
Configuración de seguridad	El estado de la configuración de seguridad muestra el nivel de seguridad definido para el cortafuegos. Haga clic en el vínculo para cambiar el nivel de seguridad.
Eventos bloqueados	El estado de los eventos bloqueados muestra el número de eventos que se han bloqueado en el día actual. Haga clic en el vínculo para ver detalles de eventos procedentes de la página Eventos entrantes.
Cambios de reglas de aplicación	El estado de las reglas de aplicación muestra el número de reglas de aplicación que han cambiado recientemente. Haga clic en el vínculo para ver la lista de aplicaciones permitidas y bloqueadas, así como para modificar los permisos de las aplicaciones.
Novedades	**Novedades** muestra la última aplicación a la que se concedió acceso pleno a Internet.
Último evento	**Último evento** muestra los eventos entrantes más recientes. Haga clic en un vínculo para rastrear el evento o definir la dirección IP como fiable. Esta última acción permitirá que todo el tráfico procedente de dicha dirección llegue hasta su equipo.
Informe diario	**Informe diario** muestra el número de eventos entrantes bloqueados por Personal Firewall en el día actual, esta semana y este mes. Haga clic en el vínculo para ver detalles de eventos procedentes de la página Eventos entrantes.
Aplicaciones activas	**Aplicaciones activas** permite ver qué aplicaciones están abiertas y con acceso a Internet en el equipo. Haga clic en una aplicación para consultar las direcciones IP a las que se está conectando.
Tareas comunes	Haga clic en un vínculo de **Tareas comunes** para ir a las páginas de Personal Firewall, donde podrá consultar la actividad del cortafuegos y llevar a cabo algunas tareas.

Para ver la página Resumen de aplicaciones:

1 Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Ver resumen.**

2 Haga clic en **Cambiar vista** y, a continuación, seleccione **Resumen de la aplicación**.

La página Resumen de la aplicación contiene los datos siguientes:

Elemento	Descripción
Control del tráfico	El **Control del tráfico** muestra el volumen de tráfico entrante y saliente en las conexiones de Internet durante los últimos quince minutos. Haga clic en el gráfico para ver los detalles de control del tráfico.
Aplicaciones activas	**Aplicaciones activas** muestra el uso de ancho de banda por parte de las aplicaciones con mayor actividad del equipo durante las últimas veinticuatro horas. **Aplicación**: aplicación que accede a Internet. **%**: porcentaje de ancho de banda utilizado por la aplicación. **Permiso**: tipo de acceso a Internet que se permite a la aplicación. **Regla creada**: fecha de creación en que se creó la regla de aplicación.
Novedades	**Novedades** muestra la última aplicación a la que se concedió acceso pleno a Internet.
Aplicaciones activas	**Aplicaciones activas** permite ver qué aplicaciones están abiertas y con acceso a Internet en el equipo. Haga clic en una aplicación para consultar las direcciones IP a las que se está conectando.
Tareas comunes	Haga clic en un vínculo de **Tareas comunes** para ir a las páginas de Personal Firewall, donde podrá consultar el estado de la aplicación y llevar a cabo algunas tareas.

Para ver la página Resumen de evento:

1 Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Ver resumen.**

2 Haga clic en **Cambiar vista** y, a continuación, seleccione **Resumen de evento**.

La página Resumen de evento contiene los datos siguientes:

Elemento	Descripción
Comparación de puertos	**Comparación de puertos** muestra un gráfico de sectores de los puertos del equipo que se han intentado abrir con mayor frecuencia durante los últimos 30 días. Haga clic en el nombre de un puerto para ver detalles de la página Eventos entrantes. También puede situar el cursor sobre el número de puerto para ver una descripción de dicho puerto.
Infractores principales	**Infractores principales** indica las direcciones IP bloqueadas con mayor frecuencia, cuándo se produjo el último evento entrante de cada dirección y el número total de eventos entrantes registrados de cada dirección en los últimos 30 días. Haga clic en un evento para ver detalles de la página Eventos entrantes.

Elemento	Descripción
Informe diario	**Informe diario** muestra el número de eventos entrantes bloqueados por Personal Firewall en el día actual, esta semana y este mes. Haga clic en un número para ver detalles de eventos procedentes del registro de eventos entrantes.
Último evento	**Último evento** muestra los eventos entrantes más recientes. Haga clic en un vínculo para rastrear el evento o definir la dirección IP como fiable. Esta última acción permitirá que todo el tráfico procedente de dicha dirección llegue hasta su equipo.
Tareas comunes	Haga clic en un vínculo de **Tareas comunes** para ir a las páginas de Personal Firewall, donde podrá consultar los detalles de los eventos y llevar a cabo algunas tareas.

Para ver la página Resumen de HackerWatch:

1 Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Ver resumen.**

2 Haga clic en **Cambiar vista** y, a continuación, seleccione **Resumen de HackerWatch**.

La página Resumen de HackerWatch contiene los datos siguientes**.**

Elemento	Descripción
Actividad mundial	**Actividad mundial** muestra un mapa mundial que identifica la actividad recién bloqueada que ha supervisado HackerWatch.org. Haga clic en el mapa para abrir el mapa de análisis de amenazas mundiales en HackerWatch.org.
Rastreo de eventos	**Seguimiento de eventos** muestra el número de eventos entrantes enviados a HackerWatch.org.
Actividad mundial de los puertos	**Actividad mundial de los puertos** muestra los puertos que han recibido un mayor número de amenazas en los últimos cinco días. Haga clic en un puerto para ver su número y descripción.
Tareas comunes	Haga clic en un vínculo de **Tareas comunes** para ir a las páginas de HackerWatch.org, donde podrá obtener información adicional sobre las actividades de piratería a escala mundial.

Información acerca de la página Aplicaciones de Internet

En la página Aplicaciones de Internet podrá consultar una lista de las aplicaciones permitidas y bloqueadas.

Para iniciar la página Aplicaciones de Internet:

- Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Aplicaciones** (Figura 2-2).

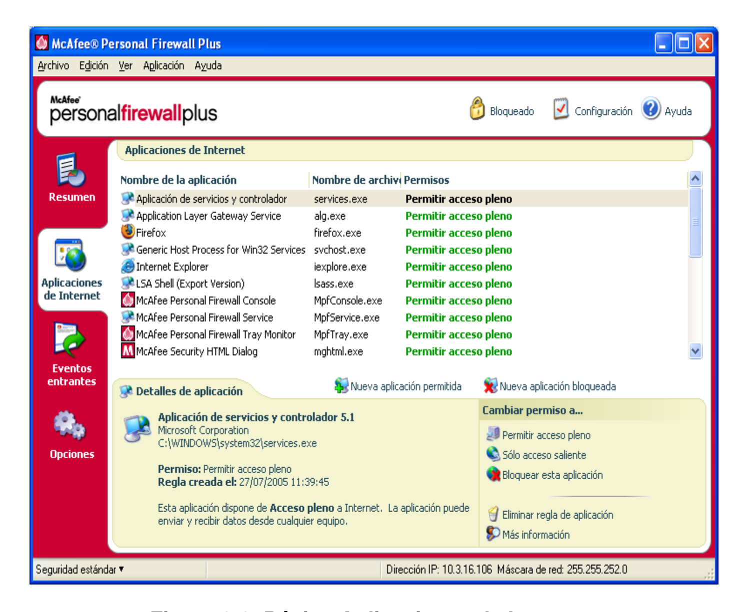


Figura 2-2. Página Aplicaciones de Internet

La página Aplicaciones de Internet contiene los datos siguientes:

- Nombres de aplicaciones
- Nombres de archivo
- Niveles de permiso actuales
- Detalles de la aplicación: nombre y versión de la aplicación, nombre de la compañía, nombre de la ruta, permiso, fechas y horas del evento y explicaciones de los tipos de permisos.

Cambio de las reglas de aplicación

Personal Firewall le permite cambiar las reglas de acceso de las aplicaciones.

Para cambiar una regla de aplicación:

1 Haga clic con el botón secundario en el icono de McAfee, seleccione **Personal Firewall** y, a continuación, seleccione **Aplicaciones de Internet**.

2 En la lista **Aplicaciones de Internet**, haga clic con el botón secundario en la regla de la aplicación de una aplicación y, a continuación, seleccione un nivel diferente:

- **Permitir acceso pleno:** permite que la aplicación establezca conexiones de Internet entrantes y salientes.
- **Sólo acceso saliente:** permite que la aplicación establezca sólo una conexión de Internet saliente.
- **Bloquear esta aplicación:** prohíbe que la aplicación acceda a Internet.

NOTA
Las aplicaciones que se han bloqueado con anterioridad, permanecerán bloqueadas cuando el cortafuegos se configura con el valor de seguridad **Abierto** o **Bloqueado**. Para evitar esto, puede cambiar las reglas de acceso de la aplicación a **Acceso pleno** o eliminar la regla del permiso **Bloqueado** en la lista **Aplicaciones de Internet**.

Para eliminar una regla de aplicación:

1 Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Aplicaciones de Internet**.

2 En la lista **Aplicaciones de Internet**, haga clic con el botón secundario en la regla de la aplicación y, a continuación, seleccione **Eliminar regla de aplicación**.

La próxima vez que la aplicación solicite acceder a Internet, será posible establecer su nivel de permiso para que se vuelva a agregar a la lista.

Permiso y bloqueo de aplicaciones de Internet

Para modificar la lista de las aplicaciones de Internet que se han bloqueado y a las que se ha permitido el acceso:

1 Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Aplicaciones de Internet**.

2 En la página Aplicaciones de Internet, haga clic en una de las siguientes opciones:

- **Nueva aplicación permitida**: permite que la aplicación acceda por completo a Internet.
- **Nueva aplicación bloqueada**: prohíbe que una aplicación acceda a Internet.
- **Eliminar regla de aplicación**: elimina una regla de aplicación.

Información acerca de la página Eventos entrantes

La página Eventos entrantes permite consultar el registro de eventos entrantes generado cuando Personal Firewall bloquea las conexiones a Internet no solicitadas.

Para abrir la página Eventos entrantes:

- Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Eventos entrantes** (Figura 2-3).

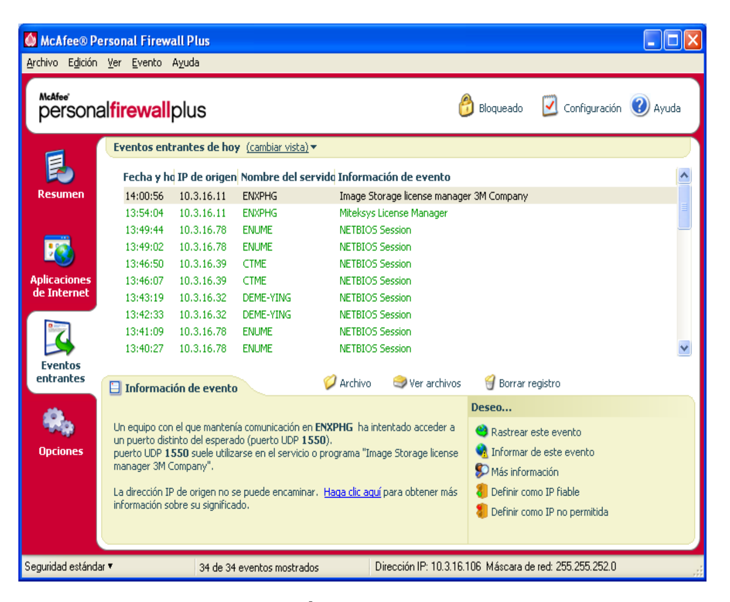


Figura 2-3. Página Eventos entrantes

La página Eventos entrantes incluye los datos siguientes:

- Fechas y horas de los eventos
- IP de origen

- Nombres de hosts
- Nombres del servicio o de la aplicación
- Detalles del evento: tipos de conexión, puertos de conexión, nombre de host o IP y explicación sobre los eventos de los puertos

Explicación de los eventos

Información acerca de las direcciones IP

Las direcciones IP están compuestas por números: para ser más exactos, cuatro números comprendidos entre 0 y 255. Estos números permiten identificar un lugar concreto al que dirigir el tráfico a través de Internet.

Tipos de direcciones IP

Existen varias direcciones IP que no se utilizan con demasiada frecuencia por diversas razones:

Direcciones IP que no se pueden enrutar: también se conocen como “espacio de IP privadas”. Estas direcciones IP no se pueden utilizar en Internet. Los bloques de direcciones IP privadas son 10.x.x.x, 172.16.x.x - 172.31.x.x y 192.168.x.x.

Direcciones IP de bucle invertido: estas direcciones se utilizan para efectuar comprobaciones. El tráfico enviado a este grupo de direcciones IP se devuelve directamente al dispositivo que haya generado el paquete. Nunca abandona el dispositivo y se utiliza principalmente para realizar comprobaciones de hardware y software. El bloque de IP de bucle de retorno es 127.x.x.x.

Dirección IP nula: se trata de una dirección no válida. Cuando se detecta, Personal Firewall indica que el tráfico utilizó una dirección IP vacía. Esto indica con frecuencia que el emisor oculta deliberadamente el origen del tráfico. El emisor no podrá recibir ninguna respuesta de tráfico a no ser que el paquete lo reciba una aplicación que comprenda su contenido, que a su vez incluya instrucciones específicas para dicha aplicación. Las direcciones que empiezan por 0 (0.x.x.x) son direcciones nulas. Por ejemplo, 0.0.0.0 sería una dirección IP nula.

Eventos desde 0.0.0.0

Si observa eventos procedentes de la dirección IP 0.0.0.0, existen dos causas probables. La primera, y más común, es que el equipo ha recibido un paquete defectuoso. Internet no es siempre fiable al 100%, por lo que puede que reciba paquetes dañados. Dado que Personal Firewall ve los paquetes antes de que se validen mediante TCP/IP, es posible que informe acerca de estos paquetes como un evento.

La otra situación se produce cuando la IP de origen está trucada o simulada. Los paquetes trucados pueden ser signos de que alguien está buscando troyanos en el equipo. Personal Firewall bloquea este tipo de actividad, por lo que su equipo estará seguro.

Eventos de 127.0.0.1

Los eventos a veces enumerarán su IP de origen como 127.0.0.1. Esto se conoce como una dirección de bucle invertido o host local.

Muchos programas habituales utilizan la dirección de bucle invertido para la comunicación entre sus componentes. Por ejemplo, se pueden configurar muchos servidores Web o servidores personales de correo a través de una interfaz Web. Para acceder a la interfaz, escriba "http://localhost/" en el navegador Web.

Personal Firewall permite el tráfico procedente de dichos programas, de modo que si detecta eventos procedentes de 127.0.0.1 es probable que la dirección IP sea simulada o trucada. Los paquetes trucados normalmente indican que otro equipo está buscando troyanos en el suyo. Personal Firewall bloquea estos intentos de intrusión, por lo que su equipo estará seguro.

Algunos programas, principalmente Netscape 6.2 y superiores, requieren que agregue 127.0.0.1 a la lista Direcciones IP fiables. Los componentes de estos programas se comunican entre sí de tal forma que Personal Firewall no puede determinar si el tráfico es local o no.

En el ejemplo de Netscape 6.2, si no confía en la dirección 127.0.0.1, no podrá utilizar su lista de contactos. Por lo tanto, si detecta tráfico procedente de 127.0.0.1 y todas las aplicaciones instaladas en su equipo funcionan con normalidad, resulta completamente seguro bloquear este tráfico. Pero si un programa (como Netscape) experimenta algún problema, coloque la dirección 127.0.0.1 en la lista de direcciones IP fiables de Personal Firewall y compruebe si se ha solucionado el problema.

Si de esta forma se soluciona el problema, debe sopesar las opciones siguientes: si confía en la dirección 127.0.0.1, el programa funcionará, pero estará más expuesto a sufrir ataques desde IP simuladas. Si no confía en esta dirección, el programa no funcionará, pero permanecerá protegido frente a determinado tráfico malintencionado.

Eventos procedentes de equipos de la LAN

Los eventos pueden originarse en equipos situados en la red de área local (LAN). Para indicar que estos eventos se originan en su red, Personal Firewall los muestra en verde.

En la mayoría de las configuraciones de redes de área local (LAN) empresariales, se debe seleccionar la opción **Confiar en todos los equipos de la LAN** en las opciones de IP fiables.

En algunas situaciones, su red "local" puede resultar tan peligrosa como Internet, especialmente si su equipo está en una red DSL de gran ancho de banda o utiliza módem por cable. En este caso, no seleccione **Confiar en todos los equipos de la LAN**. En su lugar, agregue las direcciones IP de los equipos locales a la lista de direcciones IP fiables.

Eventos procedentes de direcciones IP privadas

Las direcciones IP con formato 192.168.xxx.xxx, 10.xxx.xxx.xxx y 172.16.0.0 - 172.31.255.255 suelen denominarse direcciones IP privadas o que no se pueden enrutar. Estas direcciones IP nunca deben abandonar la red, por lo que casi siempre resultan fiables.

El bloque 192.168.xxx.xxx se utiliza con Microsoft Internet Connection Sharing (ICS). Si utiliza una red ICS, y ve eventos con este bloque, es posible que desee agregar la dirección IP 192.168.255.255 a la lista de direcciones IP fiables. De esta forma confiará en todo el bloque 192.168.xxx.xxx.

Si no se encuentra en una red privada, y ve eventos con direcciones similares, es posible que la dirección IP de origen haya sido trucada o simulada. Los paquetes trucados normalmente presentan signos de que alguien está buscando troyanos. Personal Firewall ya ha bloqueado esta dirección, por lo que su equipo estará seguro.

Dado que las direcciones IP privadas se refieren a diferentes equipos en función de la red en que se encuentren, no se informará acerca de estos eventos, ya que no serviría de nada.

Visualización de eventos en el registro de eventos entrantes

El registro de eventos entrantes muestra los eventos de diferentes maneras. La vista predeterminada se limita a los eventos que han tenido lugar el día actual. También se pueden ver los eventos que se han producido durante la semana anterior, o incluso consultar el registro completo.

Personal Firewall también permite consultar los eventos entrantes producidos en un día concreto, los procedentes de determinadas direcciones IP o los que presentan la misma información.

Para obtener información acerca de un evento, haga clic en él y visualice la información que aparecerá en el panel **Información de evento**.

Visualización de los eventos del día actual

Utilice esta opción para consultar los eventos del día.

Para visualizar los eventos del día actual:

1. Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Eventos entrantes**.
2. En el registro de eventos entrantes, haga clic con el botón secundario en una entrada y, a continuación, haga clic en **Visualizar los eventos del día actual**.

Visualización de eventos de esta semana

Utilice esta opción para consultar los eventos de la semana.

Para visualizar los eventos de esta semana:

1. Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Eventos entrantes**.
2. En el registro de eventos entrantes, haga clic con el botón secundario en una entrada y, a continuación, haga clic en **Mostrar eventos de esta semana**.

Visualización del registro completo de eventos entrantes

Utilice esta opción para consultar todos los eventos.

Para visualizar todos los eventos del registro de eventos entrantes:

1. Haga clic con el botón secundario en el icono de McAfee, seleccione la opción **Personal Firewall** y haga clic en **Eventos entrantes**.
2. En el registro de eventos entrantes, haga clic con el botón secundario en una entrada y, a continuación, haga clic en **Mostrar registro completo**.

   El registro de eventos entrantes muestra todos los eventos del registro de eventos entrantes.

Visualización de los eventos de un determinado día

Utilice esta opción para consultar los eventos de un día concreto.

Para visualizar los eventos de un día concreto:

1. Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Eventos entrantes**.
2. En el registro de eventos entrantes, haga clic con el botón secundario en una entrada y, a continuación, haga clic en **Mostrar sólo eventos de un día concreto**.

Visualización de los eventos de una dirección de Internet específica

Utilice esta opción para consultar otros eventos que se originen en una dirección de Internet determinada.

Para visualizar los eventos de una dirección de Internet:

1. Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y haga clic en **Eventos entrantes**.
2. En el registro de eventos entrantes, haga clic con el botón secundario en una entrada y, a continuación, haga clic en **Mostrar sólo eventos de una dirección de Internet concreta**.

Visualización de eventos que comparten la misma información de evento

Utilice esta opción para comprobar si existen otros eventos en el registro de eventos entrantes que presenten la misma información en la columna Información de evento que el evento seleccionado. Podrá consultar cuántas veces ha ocurrido dicho evento y si tienen el mismo origen. La columna Información de evento ofrece una descripción del evento y, si se conoce, el programa o servicio que suele utilizar dicho puerto.

Para visualizar eventos que comparten la misma información de evento:

1 Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y haga clic en **Eventos entrantes**.

2 En el registro de eventos entrantes, haga clic con el botón secundario en una entrada y, a continuación, haga clic en **Mostrar sólo eventos con la misma información de evento**.

Respuesta a eventos entrantes

Además de visualizar detalles sobre los eventos del registro de eventos entrantes, puede efectuar un rastreo visual de las direcciones IP de un evento concreto o incluso obtener detalles en el sitio Web contra la piratería HackerWatch.org.

Rastreo del evento seleccionado

Puede intentar un rastreo visual de las direcciones IP correspondientes a un evento del registro de eventos entrantes.

Para rastrear un evento seleccionado:

1 Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y seleccione **Eventos entrantes**.

2 En el registro de Eventos entrantes, haga clic con el botón secundario del ratón en el evento que desea rastrear y, a continuación, haga clic en **Rastrear evento seleccionado**. También puede hacer doble clic en el evento para rastrear un evento.

De forma predeterminada, Personal Firewall inicia un rastreo visual mediante el programa Personal Firewall Visual Trace integrado.

Obtención de consejos de HackerWatch.org

Para obtener consejos de HackerWatch.org:

1. Haga clic con el botón secundario en el icono de McAfee, seleccione la opción **Personal Firewall** y seleccione **Eventos entrantes**.
2. Seleccione la entrada del evento en la página Eventos entrantes y, a continuación, haga clic en **Obtener más información**. En el panel **Deseo**.

Se abrirá el navegador Web predeterminado y el sitio Web de HackerWatch.org para obtener información sobre el tipo de eventos y consejos sobre si debe informar al respecto.

Informes sobre un evento

Para notificar sobre un evento que considere un ataque sobre su equipo:

1. Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y seleccione **Eventos entrantes**.
2. Haga clic en el evento sobre el que desea informar y, a continuación, seleccione **Informar de este evento** en el panel **Deseo**.

Personal Firewall informa sobre el evento a HackerWatch.org mediante su identificación exclusiva.

Registro en HackerWatch.org

Al abrir la página Resumen por primera vez, Personal Firewall se pondrá en contacto con HackerWatch.org para generar la identificación exclusiva del usuario. Si ya es usuario, su registro se validará de inmediato. Si es un usuario nuevo, deberá introducir un nombre de usuario y una dirección de correo electrónico y, a continuación, hacer clic en el vínculo de validación del mensaje de correo electrónico de confirmación remitido por HackerWatch.org para poder utilizar las funciones de filtro y correo electrónico de su sitio Web.

Puede informar de eventos a HackerWatch.org sin necesidad de validar su identificación de usuario. Sin embargo, para filtrar eventos y mandarlos por correo electrónico a un amigo, deberá registrarse en el servicio.

Si se registra en este servicio, sus envíos serán rastreados y nos permitirá notificarle si HackerWatch.org necesita que haga algo más o que envíe algún tipo de información adicional. También necesitamos que se registre porque debemos confirmar toda la información recibida para que resulte de utilidad.

HackerWatch.org se compromete a mantener la confidencialidad de todas las direcciones de correo electrónico proporcionadas. Si un proveedor de servicios de Internet realiza una solicitud para obtener información adicional, dicha petición se encaminará a través de HackerWatch.org, por lo que su dirección de correo electrónico nunca se verá expuesta.

Confianza en una dirección

Puede utilizar la página Eventos entrantes para agregar una dirección IP a la lista de direcciones IP fiables para permitir una conexión permanente.

Si detecta un evento en la página Eventos entrantes que contenga una dirección IP que necesite autorizar, puede configurar Personal Firewall para que permita todas las conexiones procedentes de ella en todo momento.

Para agregar una dirección IP a la lista de IP fiables:

1. Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y seleccione **Eventos entrantes**.
2. Haga clic con el botón secundario del ratón en el evento en cuya dirección IP desee confiar y, a continuación, en **Definir IP de origen como fiable**.

Verifique que la dirección IP que muestra el cuadro de diálogo de confirmación de confianza en esta dirección es correcta y haga clic en **Aceptar**. La dirección IP se agregará a la lista de IP fiables.

Para verificar que la dirección IP se ha agregado:

1. Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y seleccione **Opciones**.
2. Haga clic en el icono **IP fiables y prohibidas** y, a continuación, haga clic en la ficha **Direcciones IP fiables**.

La dirección IP aparecerá señalada en la lista de IP fiables.

Prohibición de una dirección

Si aparece una dirección IP en el registro de eventos entrantes, indica que se ha bloqueado el tráfico procedente de dicha dirección. Por lo tanto, la prohibición de una dirección no incrementa la protección del sistema a menos que su equipo tenga abiertos, intencionadamente, determinados puertos a través de la función de servicios del sistema o que incluya una aplicación con permiso para recibir tráfico.

Agregue una dirección IP a la lista de direcciones prohibidas sólo si su equipo tiene uno o más puertos abiertos intencionadamente y tiene razones para creer que debe bloquearla.

Si detecta un evento en la página Registro de eventos entrantes que contenga una dirección IP que desee prohibir, puede configurar Personal Firewall para que rechace todas las conexiones procedentes de ella.

Puede utilizar la página Eventos entrantes, que enumera las direcciones IP de todo el tráfico entrante de Internet, para prohibir una dirección IP que sospeche es el origen de actividades de Internet no deseadas o sospechosas.

Para agregar una dirección IP a la lista de IP prohibidas:

1. Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Eventos entrantes**.
2. En la página Eventos entrantes aparecen las direcciones IP de todo el tráfico de Internet entrante. Seleccione una dirección IP y, a continuación, lleve a cabo una de las siguientes acciones:
   - Haga clic con el botón secundario en la dirección IP y, a continuación, seleccione **Definir IP de origen como no permitida**.
   - En el menú **Deseo**, haga clic en **Definir como IP no permitida**.
3. En el cuadro de diálogo Agregar regla de direcciones IP no permitidas, utilice uno o más de los siguientes parámetros para configurar la dirección de IP prohibida:
   - **Una sola dirección IP**: la dirección IP que desea prohibir. La entrada predeterminada es la dirección IP que seleccionó en la página Eventos entrantes.
   - **Una serie de direcciones IP**: las direcciones IP entre la dirección especificada en De dirección IP y la dirección IP especificada en la A dirección IP.
   - **Caducidad de la regla**: fecha y hora en la que desea que caduque esta regla de dirección IP prohibida. Seleccione los menús desplegables apropiados para seleccionar la fecha y la hora.
   - **Descripción**: Si lo desea, describa la nueva regla.
   - Haga clic en **Sí**.
4. En el cuadro de diálogo, haga clic en **Sí** para confirmar la configuración. Haga clic en **No** para volver al cuadro de diálogo Agregar regla de direcciones IP no permitidas.

Si Personal Firewall detecta un evento de una conexión de Internet prohibida, le avisará según el método especificado en la página Configuración de alertas.

Para verificar que la dirección IP se ha agregado:

1. Haga clic en la ficha **Opciones**.
2. Haga clic en el icono **IP fiables y prohibidas** y, a continuación, haga clic en la ficha **Direcciones IP no permitidas**.

La dirección IP aparecerá señalada en la lista de IP prohibidas.

Gestión del registro de eventos entrantes

Puede utilizar la página Eventos entrantes para gestionar los eventos del registro de eventos entrantes que se generan cuando Personal Firewall bloquea tráfico no solicitado de Internet.

Archivado del registro de eventos entrantes

Puede archivar el registro de eventos entrantes actual para guardar todos los eventos entrantes registrados, incluidas fechas y horas, IP de origen, nombres de host, puertos e información de eventos. Archive los registros de eventos entrantes periódicamente para evitar que el registro de eventos entrantes se haga demasiado grande.

Para archivar el registro de eventos entrantes:

1. Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Eventos entrantes**.
2. En la página Eventos entrantes, haga clic en **Archivar**.
3. En el cuadro de diálogo Archivar registro, haga clic en **Sí** para continuar con la operación.
4. Haga clic en **Guardar** para guardar el archivo en la ubicación predeterminada o bien diríjase a la ubicación en la que desea guardarlo.

Nota: De manera predeterminada, Personal Firewall archiva automáticamente el registro de Eventos entrantes. Active o desactive **Archivar automáticamente los eventos registrados** en la página Configuración de registro de eventos para activar o desactivar la opción.

Visualización del registro de eventos entrantes archivado

Puede ver todos los registros de eventos entrantes previamente archivados. El archivo guardado contiene fechas y horas, IP de origen, nombres de host, puertos e información de cada evento.

Para visualizar un registro de eventos entrantes archivado:

1. Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Eventos entrantes**.
2. En la página Eventos entrantes, haga clic en **Ver archivos**.
3. Seleccione o busque el nombre del archivo archivado y haga clic en **Abrir**.

Eliminación del registro de eventos entrantes

Puede borrar toda la información del registro de eventos entrantes.

ADVERTENCIA: Una vez borrado, el registro de eventos entrantes no podrá recuperarse. Si cree que va a necesitar el Registro de eventos en el futuro, es mejor que lo guarde en un archivo archivado.

Para eliminar el registro de eventos entrantes:

1 Haga clic con el botón secundario en el icono de McAfee, seleccione la opción **Personal Firewall** y, a continuación, seleccione **Eventos entrantes**.

2 En la página Eventos entrantes, haga clic en **Borrar registro**.

3 Haga clic en **Sí** en el cuadro de diálogo para borrar el registro.

Copia de un evento en el portapapeles

Puede copiar un evento en el portapapeles para pegarlo en un archivo de texto con el Bloc de notas.

Para copiar eventos en el portapapeles:

1 Haga clic con el botón secundario en el icono de McAfee, seleccione la opción **Personal Firewall** y, a continuación, seleccione **Eventos entrantes**.

2 Haga clic con el botón secundario del ratón en el evento del registro de eventos entrantes.

3 Haga clic en **Copiar evento seleccionado en el portapapeles**.

4 Abra el Bloc de notas.

   - Escriba `notepad` en la línea de comando o haga clic en el botón **Inicio** de Windows, señale **Programas** y, a continuación, **Accesorios**. Seleccione **Bloc de notas**.

5 Haga clic en **Editar** y, a continuación, haga clic en Pegar. El texto de evento se mostrará en el Bloc de notas. Repita este paso hasta que tenga todos los eventos necesarios.

6 Guarde el archivo del Bloc de notas en un lugar seguro.

Eliminación del evento seleccionado

Puede eliminar eventos del registro de eventos entrantes.

Para eliminar eventos del registro de eventos entrantes:

1. Haga clic con el botón secundario del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Eventos entrantes**.
2. Haga clic en la entrada de evento de la página Eventos entrantes que desee eliminar.
3. En el menú Edición, haga clic en **Eliminar evento seleccionado**. El evento se borra del registro de eventos entrantes.

Acerca de las alertas

Se recomienda familiarizarse con los distintos tipos de alertas que aparecerán al utilizar Personal Firewall. Revise los siguientes tipos de alerta que aparecen y las posibles respuestas para poder responder con seguridad a una alerta.

NOTA
Las recomendaciones sobre las alertas ayudan a decidir cómo reaccionar en cada situación. Para que las alertas incluyan recomendaciones, haga clic en la ficha **Opciones**, después en el icono **Configuración de alertas** y seleccione **Usar recomendaciones inteligentes** (valor predeterminado) o **Mostrar sólo recomendaciones inteligentes** en la lista **Recomendaciones inteligentes**.

Alertas rojas

Las alertas rojas contienen información importante que requiere atención inmediata.

- **Aplicación de Internet bloqueada:** esta alerta aparece cuando Personal Firewall bloquea el acceso a Internet de una aplicación. Por ejemplo, si aparece una alerta sobre un programa troyano, McAfee denegará automáticamente el acceso del programa a Internet y recomendará que se explore el equipo en busca de virus.
- **La aplicación desea tener acceso a Internet:** esta alerta aparece cuando Personal Firewall detecta tráfico procedente de una red o de Internet para aplicaciones nuevas.
- **Se ha modificado la aplicación:** esta alerta aparece cuando Personal Firewall detecta que se ha modificado una aplicación a la que previamente autorizó el acceso a Internet. Si ha actualizado recientemente la aplicación, debe tener cuidado a la hora de concederle permiso de acceso a Internet.

- **La aplicación desea tener acceso de servidor:** esta alerta aparece cuando Personal Firewall detecta que una aplicación a la que previamente se le concedió permiso para acceder a Internet solicita acceder a Internet como servidor.

NOTA
La configuración predeterminada de Actualizaciones automáticas de Windows XP SP2 descarga e instala actualizaciones para el sistema operativo de Windows y para otros programas de Microsoft que estén instalados en su equipo sin que reciba ningún mensaje de advertencia. Cuando se actualiza una aplicación mediante una de las actualizaciones silenciosas de Windows, aparecerá una alerta de McAfee Personal Firewall la próxima vez que se ejecute la aplicación de Microsoft.

IMPORTANTE
Debe conceder acceso a las aplicaciones que necesiten acceder a Internet para obtener actualizaciones en línea del programa (como ocurre con los servicios de McAfee) para mantenerlos al día.

Alerta de aplicación de Internet bloqueada

Si aparece una alerta sobre un programa troyano (Figura 2-4), Personal Firewall denegará automáticamente el acceso del programa a Internet y recomendará que se explore el equipo en busca de virus. Si McAfee VirusScan no se ha instalado, puede iniciar McAfee SecurityCenter.



Figura 2-4. Alerta de aplicación de Internet bloqueada

Consulte una breve descripción del evento y seleccione una de las opciones siguientes:

- Haga clic en **Más información** para obtener detalles sobre el evento del registro de eventos entrantes (consulte *Información acerca de la página Eventos entrantes* en la página 22 para obtener información detallada al respecto).
- Haga clic en **Iniciar McAfee VirusScan** para analizar el equipo en busca de virus.
- Haga clic en **Continuar con lo que estaba haciendo** si no desea aplicar otra medida aparte de la que tome Personal Firewall.
- Haga clic en **Conceder acceso saliente** para permitir una conexión saliente (**Seguridad** estricta).

Aplicación que desea obtener acceso a la alerta de Internet

Si selecciona el nivel de seguridad **Estándar** o **Estricta** en las opciones de Configuración de seguridad, Personal Firewall mostrará una alerta (Figura 2-5) cuando detecte conexiones de red o de acceso a Internet procedente de aplicaciones nuevas o modificadas.



Figura 2-5. Alerta de aplicación que desea tener acceso a Internet

Si aparece una alerta que recomienda precaución a la hora de permitir el acceso a Internet a la aplicación, haga clic en **Haga clic aquí para obtener más información** para ver información adicional de la aplicación. Esta opción aparece en la alerta sólo cuando Personal Firewall está configurado para utilizar recomendaciones inteligentes.

McAfee podría no reconocer la aplicación que intenta obtener el acceso a Internet (Figura 2-6).

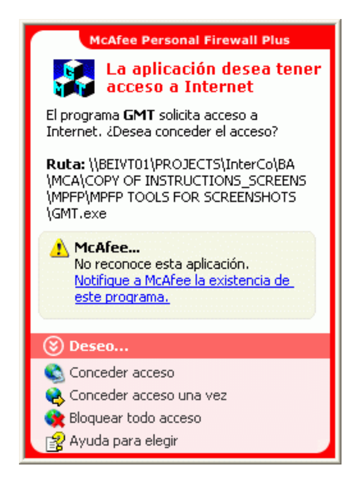


Figura 2-6. Alerta Aplicación no reconocida

Por lo tanto, McAfee no puede dar una recomendación sobre cómo gestionar la aplicación. Puede informar sobre la aplicación a McAfee haciendo clic en **Notifique a McAfee la existencia de este programa**. Aparecerá una página Web que solicitará información relacionada con la aplicación. Rellene tanta información como sea posible.

La información enviada la emplean con otras herramientas de investigación los operadores de HackerWatch para determinar si una aplicación garantiza su aparición en nuestra base de datos de aplicaciones conocidas y, si es así, el modo en que debe tratarla Personal Firewall.

Consulte una breve descripción del evento y seleccione una de las opciones siguientes:

- Haga clic en **Conceder acceso** para permitir que la aplicación establezca una conexión de Internet entrante y saliente.
- Haga clic en **Conceder acceso una vez** para permitir que la aplicación se conecte a Internet de manera temporal. El acceso se limita al tiempo desde el momento en el que se inicia la aplicación hasta cuando se cierra.
- Haga clic en **Bloquear todo acceso** para prohibir cualquier conexión a Internet.
- Haga clic en **Conceder acceso saliente** para permitir una conexión saliente (**Seguridad** estricta).
- Haga clic en **Ayuda para elegir** para ver la Ayuda en línea sobre los permisos de acceso de aplicaciones.

Alerta de modificación de aplicación

Si selecciona **Fiable**, **Estándar** o **Estricta** en las opciones de Configuración de seguridad, Personal Firewall mostrará una alerta (Figura 2-7) cuando detecte que se ha modificado una aplicación a la que se había concedido permiso de acceso a Internet. Si ha actualizado recientemente la aplicación en cuestión, debe tener cuidado a la hora de concederle permiso de acceso a Internet.



Figura 2-7. Alerta de modificación de aplicación

Consulte una breve descripción del evento y seleccione una de las opciones siguientes:

- Haga clic en **Conceder acceso** para permitir que la aplicación establezca una conexión de Internet entrante y saliente.
- Haga clic en **Conceder acceso una vez** para permitir que la aplicación se conecte a Internet de manera temporal. El acceso se limita al tiempo desde el momento en el que se inicia la aplicación hasta cuando se cierra.
- Haga clic en **Bloquear todo acceso** para prohibir cualquier conexión a Internet.
- Haga clic en **Conceder acceso saliente** para permitir una conexión saliente (seguridad **Estricta**).
- Haga clic en **Ayuda para elegir** para ver la Ayuda en línea sobre los permisos de acceso de aplicaciones.

Alerta “La aplicación desea tener acceso al servidor”

Si seleccionó el nivel de seguridad **Estricta** en las opciones de Configuración de seguridad, Personal Firewall mostrará una alerta (Figura 2-8) al detectar que una aplicación con permiso de acceso a Internet solicita acceso a Internet como servidor.



Figura 2-8. Alerta “La aplicación desea tener acceso al servidor”

Por ejemplo, aparecerá una alerta cuando MSN Messenger solicite acceso de servidor para enviar un archivo durante una sesión de chat.

Consulte una breve descripción del evento y seleccione una de las opciones siguientes:

- Haga clic en **Conceder acceso una vez** para permitir el acceso temporal a Internet de la aplicación. El acceso se limita al tiempo desde el momento en el que se inicia la aplicación hasta cuando se cierra.
- Haga clic en **Conceder acceso al servidor** para permitir que la aplicación establezca una conexión de Internet entrante y saliente.
- Haga clic en **Restringir a acceso saliente** para prohibir una conexión a Internet entrante.
- Haga clic en **Bloquear todo acceso** para prohibir cualquier conexión a Internet.
- Haga clic en **Ayuda para elegir** para ver la Ayuda en línea sobre los permisos de acceso de aplicaciones.

Alertas verdes

Las alertas verdes le notifican eventos en Personal Firewall, tales como aplicaciones a las que se les haya concedido automáticamente acceso a Internet.

Programa con permiso de acceso a Internet: esta alerta aparece cuando Personal Firewall concede acceso a Internet automáticamente a todas las aplicaciones nuevas y lo notifica con posterioridad (Seguridad **fiable**). Un ejemplo de aplicación modificada sería la que tuviera reglas modificadas que permitieran acceder automáticamente a Internet.

Alerta "Programa con permiso de acceso a Internet"

Si selecciona el nivel de seguridad **Fiable** en las opciones de Configuración de seguridad, Personal Firewall concederá acceso a Internet de forma automática a todas las aplicaciones nuevas y se lo notificará mediante una alerta (Figura 2-9).



Figura 2-9. Programa con permiso de acceso a Internet

Consulte una breve descripción del evento y seleccione una de las opciones siguientes:

- Haga clic en **Ver el registro de aplicaciones** para obtener detalles sobre el evento del registro de aplicaciones de Internet (consulte *Información acerca de la página Aplicaciones de Internet* en la página 20 para obtener información detallada al respecto).
- Haga clic en **Desactivar este tipo de alertas** para evitar la activación de alertas de este tipo.
- Haga clic en **Continuar con lo que estaba haciendo** si no desea aplicar otra medida aparte de la que tome Personal Firewall.
- Haga clic en **Bloquear todo acceso** para prohibir cualquier conexión a Internet.

Alerta de modificación de aplicación

Si selecciona el nivel de seguridad **Fiable** en las opciones de Configuración de seguridad, Personal Firewall concederá acceso a Internet de forma automática a todas las aplicaciones modificadas. Consulte una breve descripción del evento y seleccione una de las opciones siguientes:

- Haga clic en **Ver el registro de aplicaciones** para obtener detalles sobre el evento del registro de aplicaciones de Internet (consulte *Información acerca de la página Aplicaciones de Internet* en la página 20 para obtener información detallada al respecto).
- Haga clic en **Desactivar este tipo de alertas** para evitar la activación de alertas de este tipo.
- Haga clic en **Continuar con lo que estaba haciendo** si no desea aplicar otra medida aparte de la que tome Personal Firewall.
- Haga clic en **Bloquear todo acceso** para prohibir cualquier conexión a Internet.

Alertas azules

Las alertas azules contienen información, pero no requieren ninguna acción por parte del usuario.

- **Intento de conexión bloqueado:** esta alerta aparece cuando Personal Firewall bloquea tráfico no deseado procedente de una red o de Internet (Seguridad Fiable, Estándar o Estricta)

Alerta de intento de conexión bloqueado

Si ha seleccionado la seguridad **Fiable**, **Estándar** o **Estricta**, Personal Firewall muestra una alerta (Figura 2-10) al bloquear el tráfico de red o de Internet no deseado.

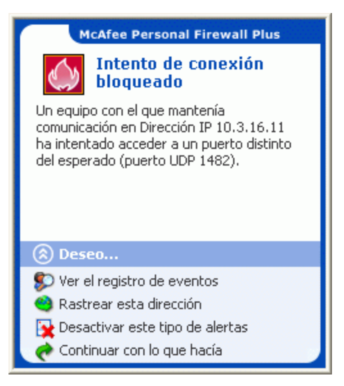


Figura 2-10. Alerta de intento de conexión bloqueado

Consulte una breve descripción del evento y seleccione una de las opciones siguientes:

- Haga clic en **Ver el registro de eventos** para obtener detalles sobre el evento del registro de eventos entrantes de Personal Firewall (consulte *Información acerca de la página Eventos entrantes* en la página 22 para obtener información detallada al respecto).
- Haga clic en **Rastrear esta dirección** para realizar un rastreo visual de las direcciones IP correspondientes al evento.
- Haga clic en **Definir como IP no permitida** para evitar que se acceda al equipo desde esta dirección. La dirección se agregará a la lista de IP no permitidas.
- Haga clic en **Definir como IP fiable** para permitir que se acceda al equipo desde esta dirección.
- Haga clic en **Continuar con lo que estaba haciendo** si no desea aplicar otra medida aparte de la que tome Personal Firewall.

Índice

P

R

T

V

W